Discrete Mathematics 310 (2010) 43–55

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the classification of perfect codes: Extended side class structures

Olof Heden [a,*], Martin Hessler [b], Thomas Westerbäck [a]

[a] Department of Mathematics, KTH, S-100 44 Stockholm, Sweden

[b] Department of Mathematics, University of Linköping, S-581 83 Linköping, Sweden

ARTICLE INFO

Article history:
Received 12 February 2007
Received in revised form 26 May 2009
Accepted 27 July 2009
Available online 12 August 2009

Keywords:
Perfect codes
Side class structures

ABSTRACT

The two 1-error correcting perfect binary codes, C and C' are said to be equivalent if there exists a permutation π of the set of the n coordinate positions and a word $\bar{d}$ such that $C' = \pi(\bar{d} + C)$. Hessler defined C and C' to be linearly equivalent if there exists a non-singular linear map φ such that $C' = \varphi(C)$. Two perfect codes C and C' of length n will be defined to be *extended equivalent* if there exists a non-singular linear map φ and a word $\bar{d}$ such that

$$C' = \varphi(\bar{d} + C).$$

Heden and Hessler, associated with each linear equivalence class an invariant L_C and this invariant was shown to be a subspace of the kernel of some perfect code. It is shown here that, in the case of extended equivalence, the corresponding invariant will be the extension of the code L_C.

This fact will be used to give, in some particular cases, a complete enumeration of all extended equivalence classes of perfect codes.

1. Introduction

A *perfect* 1*-error correcting binary code of length n* is a subset C of a direct product of the finite field Z_2

$$C \subseteq Z_2^n = Z_2 \times Z_2 \times Z_2 \times \cdots \times Z_2$$

such that for any word $\bar{x} \in Z_2^n$ there is a unique word $\bar{c} \in C$ at a distance of at most one from $\bar{x}$ where the distance between the two words $\bar{x}$ and $\bar{c}$ is defined as the number of positions in which the words $\bar{c}$ and $\bar{x}$ differ. We shall refer to such codes as *perfect codes*. It is well known and most easy to prove that the length n of a perfect code always satisfies $n = 2^m - 1$ for some integer m.

The *rank* of a perfect code C is simply the dimension of the subspace $\langle C \rangle$ of Z_2^n spanned by the words of C. The *kernel* $\ker(C)$ of a perfect code C is the set of *periods* of C:

$$\ker(C) = \{\bar{p} \in Z_2^n \mid \bar{p} + C = C\}.$$

The kernel of any code is a subspace of Z_2^n. We shall always assume that the all zero word belongs to the perfect codes that we consider and, as a consequence, the kernel of any perfect code C considered here will be a subset of C.

As in [14], we shall say that two subsets L and K of Z_2^n are *isomorphic* if there is a permutation π of the set of coordinate positions such that $\pi(L) = K$. In this case, L and K are said to be *isomorphic equivalent*, and we can consider *isomorphism equivalence classes*.

* Corresponding author.
E-mail addresses: olohed@math.kth.se (O. Heden), mahes@mai.liu.se (M. Hessler), thowest@math.kth.se (T. Westerbäck).

0012-365X/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2009.07.023

Traditional equivalence of codes (in which two codes C and C' are *equivalent* if there exists a word $\bar{d}$ and a permutation π of the set of coordinate positions such that

$$C' = \pi(\bar{d} + C),)$$

produces a very large number of equivalence classes. For example, by considering a certain construction of perfect codes, Krotov [10] gave a lower bound for the number of distinct perfect codes of length n. For example, for the length $n = 31$, his bound says that the number of distinct equivalence classes of perfect codes is at least

$$2^{2040} \cdot 3^{128}.$$

On the other hand, Hessler [9], introduced the concept of linear equivalence. Two perfect codes C and C' are *linearly equivalent* if there is a non singular automorphism φ of the vector space Z_2^n that maps the words of C onto the set of words of C':

$$\varphi(C) = C'.$$

For this type of equivalence, and in most cases, the number of equivalence classes will be relatively low. One typical example is for perfect codes of length 31, rank 27 and kernel of dimension 24, the number of linear equivalence classes is one, while the number of equivalence classes is 197; see [8,9].

One motivation for defining linear equivalence, and the related concept of extended equivalence defined below, is to bring some structure and order to the very large set of perfect codes of length greater than or equal to 31.[1] Perfect codes not related to each other by ordinary equivalence may be obtained from each other by some non singular map of the vector space Z_2^n, and may therefor still share some structural properties. For example, as is easily verified, if C and C' are linearly equivalent, then $\mathrm{rank}(C) = \mathrm{rank}(C')$ and $\dim(\ker(C)) = \dim(\ker(C'))$. So if C is any representative of some linear equivalence class $\mathcal{C}_C$ of perfect codes, then any other perfect code C' in this equivalence class $\mathcal{C}_C$ can be obtained from C simply by multiplying the words of C by some non singular $n \times n$-matrix.

Now we come to our main definition. We say that two codes C and C', both of length n, are *extended equivalent* if

$$C' = \varphi(\bar{d} + C),$$

for some automorphism φ of Z_2^n and some word $\bar{d}$. Observe that if C and C' are equivalent, or if they are linear equivalent, then they are also extended equivalent.

In [6], linear equivalence classes were characterized by subspaces of kernels of perfect codes. To every perfect code C of length n and with a kernel of dimension k was associated a linear code L_C of length $n' = 2^{n-\log(n+1)-k} - 1$. (This linear code L_C will also be described in Section 2 below.) It was shown in [6] that

(I) *For every perfect code C, the space L_C is the subspace of the kernel of some perfect code of length n',*

(II) *For every subspace L of the kernel of any perfect code of length n', there is a perfect code C of some length n such that $L = L_C$.* We prove in Section 4 that

(III) *Two perfect codes C and C' of the same length n are linearly equivalent if and only if $L_C = \pi(L_{C'})$ for some permutation π of the set of n' coordinate positions.*

Let C be any code of length n. Let $C^\star$ denote the following set of words:

$$C^\star = \{(c_1, c_2, \ldots, c_n, c_1 + c_2 + \cdots + c_n) \mid (c_1, c_2, \ldots, c_n) \in C\}. \tag{1}$$

The code $C^\star$ is called the *extended code* of C, or sometimes *the extension* of C.

In Section 4, we also show that

(IV) *Two perfect codes C and C' of the same length n are extended equivalent if and only if $L_C^\star = \pi(L_{C'}^\star)$ for some permutation π of the set of $n' + 1$ coordinate positions.*

As a consequence of this result, we will be able to describe some extended equivalence classes. For a perfect code C of length n, let $r = \mathrm{rank}(C)$ and $k = \dim(\ker(C))$. In Section 5, we enumerate the extended equivalence classes of perfect codes in the following cases:

(i) $(n, r, k) \in \{(2^m - 1, n - m + 1, n - m - \delta) \mid \delta = 2, 3, 4, 5, m = 4, 5, 6, \ldots\}$

(ii) $(n, r, k) \in \{(2^m - 1, n - m + \rho, n - m - 3) \mid \rho = 1, 2, 3, 4, m = 4, 5, 6, \ldots\}$.

[1] There is only one equivalence class of perfect codes of length 7, and those of length 15 have just recently been classified, see [11].

1.1. Some remarks on the history of perfect codes

The first perfect code was constructed by Hamming [2] in the 40's. His nice and ingenious construction is well known. Let $\mathbf{H}$ be any binary matrix of size $m \times (2^m - 1)$, which has, as columns, all possible non-zero words of length m. The set

$$C = \{\bar{c} \in Z_2^n \mid \mathbf{H}\bar{c}^{\mathrm{T}} = \bar{0}^{\mathrm{T}}\}$$

will then be a perfect code, a so-called *Hamming code*. This code is a *linear code*, i.e., a subspace of Z_2^n. All linear perfect codes of the same length are equivalent. The first non-linear perfect code was found by Vasil'ev in 1962 [15]. Now there are more than 20 distinct constructions of non-linear perfect codes, see, e.g., [14] or [5].

All possible triples of parameters (n, r, k) for which there exists a perfect code of length n, of rank r and with a kernel of dimension k, have been determined.

The dimension k of the kernel of a perfect code C of length n and of rank r must satisfy the inequality

$$k \geq \begin{cases} 2^{n-r} & \text{if } n - \log_2(n+1) + 2 \leq r \leq n \\ (n-1)/2 & \text{if } r = n - \log_2(n+1) + 1, \end{cases} \tag{2}$$

see [12]. Furthermore, the rank of any perfect code C must satisfy,

$$r \leq k + 2^{n - \log_2(n+1) - k} - 1, \tag{3}$$

see [12]. The series of papers [1,12,4], showed that for any (n, r, k) satisfying the Eqs. (2) and (3), with only a very few exceptions, there is a perfect code of length n, rank r and with a kernel of dimension k. (The exceptions are

$$(n, r, k) \in \{(15, 15, 8), (15, 15, 7), (15, 15, 6), (31, 31, 22)\}.)$$

Only a few complete enumerations of perfect codes have been presented.

For ordinary equivalence, Hergert [7] enumerated all equivalence classes of Vasil'ev codes of length $n = 15$. They all have rank equal to 12. Hessler [9] enumerated those of length $n = 31$, rank 27 and with a kernel of dimension 24. In [3] the perfect codes of length $n = 15$, rank $r = 14$ and with kernels of dimension $k = 8$, and those of length $n = 31$, rank $r = 30$ and with a kernel of dimension $k = 23$, were enumerated.

Further classifications of perfect codes of length 15 and extended perfect codes of length 16 have been performed, using computers, by Zinoviev and Zinoviev [16–18]. Finally, a complete enumeration of all perfect codes of length 15, also using computers, was given by Östergård and Pottonen [11].

1.2. Some further terminology

A *code of length n* is just a subset Q of Z_2^n. A code Q is said to be *aperiodic* if Q has no non-trivial periods $\bar{p} \neq \bar{0}$.[2]

The *weight* $w(\bar{x})$ of a word $\bar{x}$ is the number of non-zero coordinates of $\bar{x}$.

As we consider subspaces of a vector space Z_2^n over the finite field Z_2 we can define their dual spaces. Let the *dot-product* of two vectors $\bar{u} = (u_1, \ldots, u_n)$ and $\bar{v} = (v_1, \ldots, v_n)$ be defined by

$$\bar{u} \cdot \bar{v} = u_1 v_1 + \cdots + u_n v_n.$$

Then the dual space $Q^{\perp}$ of the subspace Q of Z_2^n is defned as the set of words

$$Q^{\perp} = \{\bar{x} \in Z_2^n \mid \bar{x} \cdot \bar{u} = 0 \text{ for all } \bar{u} \in Q\}.$$

The general linear group over the finite vector space Z_2^n is denoted by $GL(n, 2)$.

2. Linear equivalence, side class structure and equivalence

As already mentioned in the introduction, two perfect codes C and C', both of length n, are said to be *linearly equivalent* if there exists a non-singular linear map φ from Z_2^n to Z_2^n that maps the set of words of the code C to the set of words C'. It will be useful to consider the representation of φ by a non singular matrix $\mathbf{A}$, i.e., if $\varphi(\bar{x}) = \bar{y}$ then

$$\bar{y}^{\mathrm{T}} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \mathbf{A} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad \bar{x} = (x_1, x_2, \ldots, x_n) \in Z_2^n.$$

[2] It must perhaps be remarked that every perfect code has at least one non-trivial period, see, eg, [14] for more references on this point.

Thus, if we let $\mathbf{C}$ and $\mathbf{C}'$ denote the matrices whose columns are the words of C, respectively, C', then C and C' are linearly equivalent if and only if there exists a non-singular matrix $\mathbf{A}$ and a permutation matrix $\mathbf{P}$ (a matrix that changes only the order of the columns), of appropriate sizes, such that

$$\mathbf{C}' = \mathbf{ACP}.$$

Hessler, in [8], showed that, to decide whether or not two perfect codes are linearly equivalent, it is sufficient to consider their side class structures. To define that concept, we use the following property of a perfect code.

Clearly C is the union of pairwise disjoint cosets of the kernel of C:

$$C = \bigcup_{i=1}^{t} (\bar{c}_i + \ker(C)). \tag{4}$$

Let $\{\bar{g}_1, \ldots, \bar{g}_r\}$ be a basis of $\langle C\rangle$, and $\{\bar{g}_1, \ldots, \bar{g}_k\}$ be a basis of its subspace $\ker(C)$.

Any one of the coset representatives $\bar{c}_i$, $i = 1, 2, \ldots, t$, belongs to C, and may thus be expressed as a linear combination of the above set of basis vectors:

$$\bar{c}_i = \lambda_1^{(i)}\bar{g}_1 + \lambda_2^{(i)}\bar{g}_2 + \cdots + \lambda_k^{(i)}\bar{g}_k + \lambda_{k+1}^{(i)}\bar{g}_{k+1} + \cdots + \lambda_r^{(i)}\bar{g}_r, \quad i = 1, 2, \ldots, t.$$

The *side class structure* of the perfect code C is the set of words

$$Q = \left\{ \begin{pmatrix} \lambda_{k+1}^{(1)} \\ \lambda_{k+2}^{(1)} \\ \vdots \\ \lambda_r^{(1)} \end{pmatrix}, \quad \begin{pmatrix} \lambda_{k+1}^{(2)} \\ \lambda_{k+2}^{(2)} \\ \vdots \\ \lambda_r^{(2)} \end{pmatrix}, \quad \ldots, \quad \begin{pmatrix} \lambda_{k+1}^{(t)} \\ \lambda_{k+2}^{(t)} \\ \vdots \\ \lambda_r^{(t)} \end{pmatrix} \right\}, \tag{5}$$

where

$$t = \frac{|C|}{|\ker(C)|} = 2^{n-\log_2(n+1)-\dim(\ker(C))}.$$

Observe that different choices of base vectors for the linear span $\langle C\rangle$ will give different side class structures of the same perfect code C. However, Hessler [8] proved the following theorem.

Theorem 1. *Two perfect codes C and C' of the same length, with side class structures Q respectively Q', are linearly equivalent if and only if there exists an automorphism φ of Z_2^{r-k} that maps the set Q onto the set Q', i.e., $\varphi(Q) = Q'$.*

It was proved in [6] that, if the *non zero* columns of any side class structure Q of a perfect code C are placed as columns in a matrix $\mathbf{Q}$, then the row space of this matrix will be the dual space of some subspace L_C of the kernel of some perfect code of length $t - 1$. We also recall from [6] that

$$\operatorname{rank}(C) = n - \log_2(n+1) + \rho \Longrightarrow \dim(L_C) = t - 1 - \log_2(t) - \rho.$$

The next theorem was also proved in [6].

Theorem 2. *If the rows of the matrix M span the dual space of a subspace L_C of the kernel of some perfect code, and if the set of columns of M plus the zero column constitutes an aperiodic set, then this set of columns together with the zero column constitute the side class structure of some perfect code C.*

For any permutation π of the set of coordinate positions $\{1, 2, \ldots, n\}$, we define

$$\pi((c_1, c_2, \ldots, c_n)) = (c_{\pi^{-1}(1)}, c_{\pi^{-1}(2)}, \ldots, c_{\pi^{-1}(n)}),$$

and for any code C,

$$\pi(C) = \{\pi(\bar{c}) \mid \bar{c} \in C\}.$$

We note that for any such permutation π, there is a permutation matrix $\mathbf{P}$ such that

$$\bar{c}' \in \pi(C) \Leftrightarrow \bar{c}' = \mathbf{P}\bar{c} \quad \text{where } \bar{c} \in C,$$

where the words of the code C are considered as column vectors.

Hence, trivially, for any permutation π of the set of coordinate positions $\{1, 2, 3, \ldots, n\}$ and any perfect code of length n, the perfect codes C and $\pi(C)$ are linearly equivalent. Observe that equivalent perfect codes might not be linearly equivalent; in fact, it might happen that for only some words $\bar{c}$ of C the codes $\bar{c} + C$ and C are linearly equivalent. We illustrate this fact with an example.

Example. Consider the following set of columns:

$$Q = \left\{ \begin{pmatrix}0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\end{pmatrix} \right\}.$$

If we place the seven non-zero columns above as the columns in a 4×7-matrix, then we note that the row space will be the dual space of a subspace of a Hamming code of length $n = 7$. Furthermore, the set Q above is aperiodic. Hence, from the results of [6], it follows that the set of columns above is the side class structure of some perfect code C.

Now let $\bar{c}$ be a word of C in the coset of the kernel of C that corresponds to the column $(0\ 0\ 1\ 1)^{\mathrm{T}}$. Explicitly, this means that there is a set of basis vectors $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_r$ of the linear span $\langle C\rangle$ of C such that $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_{r-4}$ is a set of basis vectors for the kernel of C, and such that the word $\bar{c} = \bar{g}_{r-1} + \bar{g}_r$ belongs to C. If we add $\bar{c}$ to all the words of C we get a perfect code $\bar{c} + C$ with the side class structure

$$Q' = \left\{ \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\\1\end{pmatrix} \right\}.$$

It is easy to verify that there is no nonsingular linear map that maps Q onto the set Q'. Hence, the codes C and $\bar{c} + C$ are not linearly equivalent.

3. Extended side class structure

Consider the side class structure Q of a perfect code C, as defined in Eq. (5). To get the extended side class structure, we just add a top row, consisting only of the element 1, above the matrix consisting of the columns of the side class structure. Explicitly, if C has the side class structure Q as described in (5), then the *extended side class structure* $Q^\star$ *of* C is

$$Q^\star = \left\{ \begin{pmatrix}1\\ \lambda_{k+1}^{(1)}\\ \lambda_{k+2}^{(1)}\\ \vdots\\ \lambda_r^{(1)}\end{pmatrix}, \begin{pmatrix}1\\ \lambda_{k+1}^{(2)}\\ \lambda_{k+2}^{(2)}\\ \vdots\\ \lambda_r^{(2)}\end{pmatrix}, \quad \ldots, \quad \begin{pmatrix}1\\ \lambda_{k+1}^{(t)}\\ \lambda_{k+2}^{(t)}\\ \vdots\\ \lambda_r^{(t)}\end{pmatrix} \right\}.$$

As for perfect codes, we will say that two subsets C and C' of Z_2^n are linearly equivalent if there exists a non singular linear map φ of the vector space Z_2^n such that

$$C' = \{\varphi(c) \mid c \in C\}.$$

Lemma 1. *For any perfect code C and any word $\bar{c}$ of C, the extended side class structures of C and $\bar{c} + C$ are linearly equivalent.*

Proof. Consider the partition (4) of C into cosets the kernel of C. For any word $\bar{c}$ of C, the corresponding partition of $\bar{c} + C$ into cosets of its kernel, is

$$\bar{c} + C = \bigcup_{i=1}^{t} (\bar{c} + \bar{c}_i + \ker(\bar{c} + C)). \tag{6}$$

We note that $\langle \bar{c} + C\rangle = \langle C\rangle$ and $\ker(C) = \ker(\bar{c} + C)$. Let $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_r$ be the basis vectors of $\langle C\rangle$ that were used in the definition of the side class structure Q. As $\bar{c}$ belongs to one of the cosets of the kernel of the perfect code C, we deduce that

$$\bar{c} = \gamma_1\bar{g}_1 + \gamma_2\bar{g}_2 + \cdots + \gamma_k\bar{g}_k + \lambda_{k+1}^{(i)}\bar{g}_{k+1} + \lambda_{k+2}^{(i)}\bar{g}_{k+2} + \cdots + \lambda_r^{(i)}\bar{g}_r,$$

where $(\lambda_{k+1}^{(i)}, \lambda_{k+2}^{(i)}, \ldots, \lambda_r^{(i)})^{\mathrm{T}} \in Q$, and $(\gamma_1, \gamma_2, \ldots, \gamma_k) \in Z_2^k$.

From (6), it now follows that the extended side class structure of $\bar{c} + C$ is

$$\left\{ \begin{pmatrix}1\\ \lambda_{k+1}^{(1)}\\ \lambda_{k+2}^{(1)}\\ \vdots\\ \lambda_r^{(1)}\end{pmatrix} + \begin{pmatrix}0\\ \lambda_{k+1}^{(i)}\\ \lambda_{k+2}^{(i)}\\ \vdots\\ \lambda_r^{(i)}\end{pmatrix}, \begin{pmatrix}1\\ \lambda_{k+1}^{(2)}\\ \lambda_{k+2}^{(2)}\\ \vdots\\ \lambda_r^{(2)}\end{pmatrix} + \begin{pmatrix}0\\ \lambda_{k+1}^{(i)}\\ \lambda_{k+2}^{(i)}\\ \vdots\\ \lambda_r^{(i)}\end{pmatrix}, \quad \ldots, \quad \begin{pmatrix}1\\ \lambda_{k+1}^{(t)}\\ \lambda_{k+2}^{(t)}\\ \vdots\\ \lambda_r^{(t)}\end{pmatrix} + \begin{pmatrix}0\\ \lambda_{k+1}^{(i)}\\ \lambda_{k+2}^{(i)}\\ \vdots\\ \lambda_r^{(i)}\end{pmatrix} \right\}.$$

Note that the automorphism φ of Z_2^{r-k+1}, that can be described by multiplication with the non singular matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ \lambda_{k+1}^{(i)} & 1 & 0 & 0 & \cdots & 0 \\ \lambda_{k+2}^{(i)} & 0 & 1 & 0 & \cdots & 0 \\ \lambda_{k+3}^{(i)} & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \lambda_{r}^{(i)} & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

maps $Q^\star$ to the extended side class structure of the code $\bar{c} + C$. □

As two codes C and C' of length n are extended equivalent (see the introduction) if there is an automorphism φ of Z_2^n and a word $\bar{d}$ such that $C' = \varphi(\bar{d} + C)$, the following proposition follows immediately from the previous lemma.

Proposition 1. *Two perfect codes C and C' are extended equivalent if and only if their extended side class structures are linearly equivalent.*

As already mentioned, it was shown in [6] that if the non-zero columns of any side class structure Q are placed as columns in a matrix $\mathbf{Q}$ then the row space of $\mathbf{Q}$ is the dual space of a subspace of the kernel of some perfect code. There is a corresponding result for extended side class structures.

To prove this correspondence, we will use the following lemma.

Lemma 2. *For any code C there is an injective linear map $\varphi : Z_2^n \to Z_2^{n+1}$, such that $\varphi(C)$ equals the extended code $C^\star$.*

Proof. The lemma follows immediately from the definition of the extension of a code in (1). □

Lemma 3. *If the set of columns of the matrix $\mathbf{Q}^\star$ constitutes an extended side class structure of some perfect code, then the dual space $L^\star$ of the row space of this matrix $\mathbf{Q}^\star$ is a subspace of the kernel of some extended perfect code.*

Proof. Delete the first row and the zero column of the matrix $\mathbf{Q}^\star$. By a rather technical construction, it can be shown that the row space of the matrix $\mathbf{Q}$ constitutes the dual space of some subspace L of the kernel of some perfect code C, see [6]. Without loss of generality, we can assume that the zero column is the last column in the matrix $\mathbf{Q}^\star$.

We observe that if we let $C^\star$, $\ker(C)^\star$ and $L^\star$ denote the extensions of the codes C, $\ker(C)$ and L (see Eq. (1)), then $L^\star$ is a subspace of $\ker(C)^\star$, and the kernel of $C^\star$ is $\ker(C)^\star$. Furthermore, we get from Lemma 2 that

$$\dim(L^\star) = \dim(L). \tag{7}$$

All words of $L^\star$ have even weights, and hence the word 111...1 consisting of all 1's belongs to the dual space of $L^\star$. Consequently, by using the Eq. (7) given above, the fact that

$$\operatorname{rank}(\mathbf{Q}^\star) = \operatorname{rank}(\mathbf{Q}) + 1$$

and that all the rows in $\mathbf{Q}^\star$, apart from the row of all ones, have a zero in the last position, we may conclude that $L^\star$ is the dual space of the row space of the matrix $\mathbf{Q}^\star$. □

4. More on the dual space of an extended side class structure

Given any perfect code C with side class structure Q, let L_C denote the dual space of the row space of a matrix $\mathbf{Q}$, which has as columns the non-zero columns of Q. Note that L_C depends on the choice of both Q and the ordering of the columns of $\mathbf{Q}$.

Theorem 3. *For any perfect code C containing the zero word, and for any $\varphi \in GL(n, 2)$, there is a permutation π of the set of coordinate positions such that*

$$L_{\varphi(C)} = \pi(L_C).$$

Proof. For any two perfect codes C and C', that are linearly equivalent, there exist, by Theorem 1, a non singular matrix $\mathbf{A}$ and a permutation matrix $\mathbf{P}$ such that

$$\mathbf{AQ} = \mathbf{Q}'\mathbf{P}, \tag{8}$$

where $\mathbf{Q}$ and $\mathbf{Q}'$ are the matrices obtained in the usual way from the side class structures of the perfect codes C and C'. We note that

$$L_C = \{\bar{d} \mid \mathbf{Q}\bar{d}^{\mathrm{T}} = 0\} \quad \text{and} \quad L_{C'} = \{\bar{d} \mid \mathbf{Q}'\bar{d}^{\mathrm{T}} = 0\}. \tag{9}$$

As $\mathbf{A}$ is nonsingular, it follows from the above two relations (8) and (9) that

$$\bar{d} \in L_C \quad \Leftrightarrow \quad \mathbf{Q}\bar{d}^{\mathrm{T}} = \bar{0} \quad \Leftrightarrow \quad \mathbf{A}^{-1}\mathbf{Q}'\mathbf{P}\bar{d}^{\mathrm{T}} = \bar{0} \quad \Leftrightarrow \quad \mathbf{Q}'\mathbf{P}\bar{d}^{\mathrm{T}} = \bar{0} \quad \Leftrightarrow \quad \bar{d}\mathbf{P}^{\mathrm{T}} \in L_{C'}. \quad \square$$

Theorem 4. *For any perfect code C of length n, any word $\bar{c} \in C$ and any linear automorphism φ of Z_2^n, there is a permutation π of the set of coordinate positions such that*

$$L^{\star}_{\varphi(\bar{c}+C)} = \pi(L^{\star}_C).$$

Recall that for any perfect code C, where the set of columns in the matrix $\mathbf{Q}$ is the extended side class structure of C, $L^{\star}_C$ denotes the dual space of the row space of $\mathbf{Q}^{\star}$.

Proof. By Lemma 1, the extended perfect codes C and $C + c$ have linearly equivalent extended side classes; hence, the theorem follows by the same proof as in Theorem 3. $\square$

The conclusion to be drawn from the above proof and from [6] must be that, for the purpose of enumerating perfect codes, it will be especially useful to find the isomorphism equivalence classes of subspaces of the kernels of extended perfect codes.

5. Some examples

5.1. Extended equivalence of shortened extended perfect codes

It is well known that, if you remove any coordinate positions from an extended perfect code $C^{\star}$ of length $n = 2^m$, you get a perfect code of length $n = 2^m - 1$. Depending on which coordinate position you remove, you may get non-equivalent perfect codes. However, as we will prove below, they are linearly equivalent.

We use the following notation. If $C^{\star}$ is an extended perfect code of length n, let $C(i)^{\star}$ denote the perfect code of length $n - 1$ that we obtain by deleting the position i:

$$C(i)^{\star} = \{(c_1, c_2, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \in Z_2^{n-1} \mid (c_1, c_2, \ldots, c_{i-1}, c_i, c_{i+1}, \ldots, c_n) \in C^{\star}\}.$$

Proposition 2. *For any extended perfect code $C^{\star}$ and any $i, j \in \{1, 2, \ldots, n\}$, the two perfect codes $C(i)^{\star}$ and $C(j)^{\star}$ are linearly equivalent.*

Proof. Note that for any $i = 1, 2, \ldots, n$,

$$C^{\star} = \left\{ \left(c_1, \ldots, c_{i-1}, \sum_{v \neq i} c_v, c_{i+1}, \ldots, c_n \right) \middle| \, (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \in C(i)^{\star} \right\}.$$

From Lemma 2, we deduce that there are bijective linear maps φ_i and φ_j from Z_2^n onto the space of words of even weight of Z_2^{n+1} such that

$$\varphi_i(C(i)^{\star}) = C^{\star} \quad \text{and} \quad \varphi_j(C(j)^{\star}) = C^{\star}.$$

The map $\varphi_i^{-1} \circ \varphi_j$ will thereby be a non-singular linear map ψ of Z_2^n, and

$$\psi(C(j)^{\star}) = \varphi_i^{-1} \circ \varphi_j(C(j)^{\star}) = \varphi_i^{-1}(C^{\star}) = C(i)^{\star},$$

which proves the lemma. $\square$

It is important to remark that V.A. Zinoviev and D.V. Zinoviev in [17] gave a necessary and sufficient condition for the perfect codes $C(i)^{\star}$ and $C(j)^{\star}$ to be equivalent.

5.2. Notation and a general result

Next, we shall enumerate the extended equivalence classes of perfect codes of length n with a kernel of dimension $n - \log_2(n + 1) - 3$, and the extended equivalence classes of perfect codes of length n and rank $n - \log_2(n + 1) + 1$, for some specific values of the dimension of the kernel of C.

We first need to define some notation: for any subspace L of an extended Hamming code of length $m = 2^{\delta}$, let $\mathbf{Q}(L)$ denote a matrix whose rows consist of a base of generators for the dual space of L, and whose first row is the word of all 1's. Let $Q(L)$ denote the set of columns you get by deleting the first row of the matrix $\mathbf{Q}(L)$. We illustrate the notation by an example that will also be used later.

Example. Let C be the extended Hamming code

$$C = \langle 11110000, 11001100, 10101010, 11111111\rangle.$$

The parity check matrix of this code is the matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

If we define the space $L^{\star}_{C_5}$ to be equal to

$$L^{\star}_{C_5} = \langle 11111111, 11110000, 11001100\rangle,$$

then the matrix $\mathbf{Q}(L^{\star}_{C_5})$ is

$$\mathbf{Q}(L^{\star}_{C_5}) = \left(\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right),$$

and the set $Q(L^{\star}_{C_5})$ is

$$Q(L^{\star}_{C_5}) = \left\{ \begin{pmatrix} 0\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\1\\1 \end{pmatrix} \right\}.$$

Proposition 3. *The number of extended equivalence classes of perfect codes of length n, of rank $n - \log_2(n+1) + \rho$, where $\rho = 1$ or 2, and with a kernel of dimension $n - \log_2(n+1) - \delta$, is equal to the number of isomorphism equivalence classes of subspaces $L^{\star}$ of dimension $m - \log_2(m+1) - \rho$ of extended Hamming codes of length $m+1 = 2^{\delta}$ with aperiodic set $Q(L^{\star})$.*

Note that the set $Q(L^{\star}_{C})$ in the example above is not aperiodic. The word $(0 \quad 0 \quad 1 \quad 0)^{\mathrm{T}}$ is a period. Thus, the space $L^{\star}_{C_5}$ does not contribute to the set of extended equivalence classes of perfect codes of length n with kernels of dimension $n - \log_2(n+1) - 3$ and of rank $n - \log_2(n+1) + 1$.

(Let us remark that the proposition above only will be used below in the case $\rho = 1$.)

Proof. Consider the $(\rho+\delta+1)\times 2^{\delta}$-matrix $\mathbf{Q}^{\star}$ obtained from the extended side class structure of a perfect code. By Lemma 3, the dual space of the row space of $\mathbf{Q}^{\star}$ is a subspace $L^{\star}$ of the kernel of some extended perfect code $C^{\star}$ of length $m+1 = 2^{\delta}$. As the rows of the matrix $\mathbf{Q}^{\star}$ are linear independent, we get that

$$\dim(L^{\star}) = 2^{\delta} - \rho - \delta - 1.$$

By Lemma 2, the subspace $L^{\star}$ of $C^{\star}$ is isomorphic to a subspace L of a perfect code $C = C(i)^{\star}$, for any i. The length of C is $m = 2^{\delta} - 1$ and the dimension L is $m - \log_2(m+1) - \rho$, where ρ equals 1 or 2. This implies (see, e.g., [6]), that C is a Hamming code. Thus $L^{\star}$ must be a subspace of an extended Hamming code. By Theorem 4, the proposition follows. □

5.3. Enumeration where the kernel has dimension $n - \log_2(n+1) - 3$

Proposition 4. *The number of extended equivalence classes of perfect codes C of length $n = 2^m - 1$ and with a kernel of dimension $n - \log_2(n+1) - 3$ will be equal to 1 in case the rank of C equals $n - \log_2(n+1) + 4$ or $n - \log_2(n+1) + 1$. In the case the rank equals $n - \log_2(n+1) + 2$ or $n - \log_2(n+1) + 3$ the number of extended equivalence classes of perfect codes will be equal to 2.*

We should remark here that it follows from (3) that in case the kernel of a perfect code C of length n has dimension equals $n - \log_2(n+1) - 3$, then the rank of C cannot be greater than $n - \log_2(n+1) + 4$.

Proof. The number of extended equivalence classes of perfect codes C, with kernels of dimension 3 is equal, by a combination of Lemma 3 and Theorem 4, to the number of isomorphism equivalence classes of subspaces of kernels of extended perfect codes of length 8 and of dimension ρ, where

$$\rho = n - \log_2(n+1) + 4 - \mathrm{rank}(C).$$

In the case where the rank of C equals $n - \log_2(n+1) + 4$, then there is only one extended equivalence class, as any linear code has exactly one subspace of dimension zero.

For the remaining cases, we may, without loss of generality, assume that C equals the following linear span:

$$C = \langle 11111111, 11110000, 11001100, 10101010\rangle.$$

By examining the words of the code C, we see that there are two isomorphism equivalence classes of subspaces of dimension 1. The subspaces $L^\star_{C_1}$ and $L^\star_{C_2}$ below are representatives of these two equivalence classes:

$$L^\star_{C_1} = \langle 11111111\rangle,$$
$$L^\star_{C_2} = \langle 11110000\rangle.$$

The row spaces of the matrices $\mathbf{Q}(L^\star_{C_1})$ and $\mathbf{Q}(L^\star_{C_2})$ below are the dual spaces of these subspaces:

$$\mathbf{Q}(L^\star_{C_1}) = \left(\begin{array}{cccccccc} 1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1\\ \hline 0&0&0&0&0&0&1&1\\ 0&0&0&0&0&1&0&1\\ 0&0&0&1&0&0&0&1 \end{array}\right) \quad \text{resp.} \quad \mathbf{Q}(L^\star_{C_2}) = \left(\begin{array}{cccccccc} 1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1\\ \hline 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&1\\ 0&0&0&0&0&1&0&1 \end{array}\right).$$

As can be easily checked, both of the sets $Q(L^\star_{C_1})$ and $Q(L^\star_{C_2})$ are aperiodic sets. Thus the number of extended equivalence classes in this case is equal to two.

The number of isomorphism equivalence classes of subspaces of dimension two is also equal to 2. It is not very difficult to check that any such subspace is isomorphic to either $L^\star_{C_3}$ or $L^\star_{C_4}$ below:

$$L^\star_{C_3} = \langle 11111111, 00001111\rangle,$$
$$L^\star_{C_4} = \langle 11110000, 11001100\rangle.$$

These subspaces are not isomorphic, as there is trivially no permutation π such that $\pi(11111111) \in L^\star_{C_4}$.

In this case, we get the matrices

$$\mathbf{Q}(L^\star_{C_3}) = \left(\begin{array}{cccccccc} 1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1\\ \hline 0&0&0&0&0&0&1&1\\ 0&0&0&0&0&1&0&1 \end{array}\right) \quad \text{resp.} \quad \mathbf{Q}(L^\star_{C_4}) = \left(\begin{array}{cccccccc} 1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1\\ \hline 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&1 \end{array}\right).$$

As in the previous case, we thus get two extended equivalence classes.

Similarly, in the case of subspaces of dimension three, there are just two isomorphism equivalence classes of subspaces of dimension three of a Hamming code of length 8: the linear span $L^\star_{C_5}$ discussed in the above example, and the span $L^\star_{C_6}$ below:

$$L^\star_{C_6} = \langle 11110000, 11001100, 10101010\rangle.$$

The corresponding matrix is

$$\mathbf{Q}(L^\star_{C_6}) = \left(\begin{array}{cccccccc} 1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1\\ \hline 0&0&0&0&0&0&0&1 \end{array}\right).$$

The set of columns $Q(L^\star_{C_6})$ is aperiodic. As the set of columns $Q(L^\star_{C_5})$ is not aperiodic (see the above example), we conclude that there is only one extended equivalence class of perfect codes in this case. □

5.4. Enumeration in case of rank $n - \log_2(n+1) + 1$

We will use a computer search for the calculation of the number of extended equivalence classes of perfect codes of length n, of rank $n - \log_2(n+1) + 1$ and with kernels of dimension $n - \log_2(n+1) - 4$ and $n - \log_2(n+1) - 5$, respectively. In this search, we shall apply Proposition 3, so we have to calculate the number of isomorphism equivalence classes of subspaces L of dimension $m - \log_2(m+1) - 1$, of extended Hamming codes of length $m + 1 = 2^\delta$, where $n - \log_2(n+1) - \delta$ equals the dimension of the kernel of perfect codes that we are to enumerate. In the computer search, we will thus consider extended Hamming codes of lengths 16 and 32.

Recall that here the two subspaces L and L' of Z_2^{m+1} are isomorphic if there is a permutation π of the set of $m+1$ coordinate positions such that $\pi(L) = L'$. We will thus enumerate all isomorphism equivalence classes of vector spaces L satisfying

(D) *L is a subspace of dimension $m - \log_2(m+1) - 1$ of some extended Hamming code H of length $m+1$, where $m+1 = 16$ and 32, respectively*,

(A) The set of columns $Q(L)$ *constitutes an aperiodic set*.

Since given any two Hamming codes H and H' of the same length $m+1$, there is a permutation π of the set of coordinate positions such that $\pi(H) = H'$, we immediately get the following lemma:

Lemma 4. *The number of isomorphism equivalence classes of spaces L satisfying the conditions (D) and (A) above equals the number of isomorphism equivalence classes of subspaces of dimension $m - \log_2(m+1) - 1$ of some particular Hamming code H of length $m+1$ satisfying the condition (A).*

We start our investigations by observing that any subspace of dimension $m - \log_2(m+1) - 1$ of an extended Hamming code of length $m+1$ must be isomorphic to the dual space of the row space of a $(\log_2(m+1)+2) \times (m+1)$-matrix

$$\mathbf{Q}(L) = \left[\begin{array}{cccccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & \cdots & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 0 \\ \hline x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & \cdots & x_{m-2} & x_{m-1} & x_m & x_{m+1} \end{array}\right], \tag{10}$$

for some non zero word $\bar{x} = (x_1, x_2, x_3, x_4, \ldots, x_{m+1}) \in Z_2^{m+1}$. Note that the dual space of L is the union of the dual space $H^\perp$ of the Hamming code H and a coset $\bar{x} + H^\perp$. Now consider the possibilities for the coset representative $\bar{x}$ of $H^\perp$ in Z_2^{m+1}.

Let H denote the extended Hamming code of length $m+1$, which is the dual space of the space $H^\perp$ generated by the first $\log_2(m+1)+1$ rows of the matrix $\mathbf{Q}(L)$ above. Let $\bar{e}_{m+1}$ and $\bar{e}_{\{m,m+1\}}$ denote the words

$$\bar{e}_{m+1} = 000\ldots001 \quad \text{respectively} \quad \bar{e}_{\{m,m+1\}} = 000\ldots0011,$$

and likewise for the words $\bar{e}_i$ and $\bar{e}_{\{j,m+1\}}$ for $i = 1, 2, 3, \ldots, m$ and $j = 1, 2, 3, \ldots, m-1$.

Lemma 5. *Any subspace L of dimension $m - \log_2(m+1) - 1$ of an extended Hamming code of length $m+1$ is isomorphic to a subspace that has as dual space the space generated by the rows in the matrix $\mathbf{Q}(L)$ above, where the word $\bar{x}$ belongs to one of the sets $H \setminus H^\perp$, $H + \bar{e}_{m+1}$ or $H + \bar{e}_{\{m,m+1\}}$.*

Proof. As H is an extended perfect code, we know that

$$Z_2^{m+1} = H \cup (H + \bar{e}_1) \cup \cdots \cup (H + \bar{e}_{m+1}) \cup (H + \bar{e}_{\{1,m+1\}}) \cup (H + \bar{e}_{\{2,m+1\}}) \cup \ldots \cup (H + \bar{e}_{\{m,m+1\}}).$$

For any extended Hamming code H and any i_1, i_2 there is a permutation π of the set of coordinate positions such that $\pi(H) = H$, $\pi(i_1) = m$ and $\pi(i_2) = m+1$. Now, if $\bar{x} \in H + \bar{e}_{\{i_1,i_2\}}$ then $\bar{x} = \bar{h} + \bar{e}_{\{i_1,i_2\}}$ for some word $\bar{h}$ of H. As in general, $\pi(\bar{a} + \bar{b}) = \pi(\bar{a}) + \pi(\bar{b})$, we get that

$$\pi(\bar{x}) = \pi(\bar{h}) + \bar{e}_{\{m,m+1\}},$$

where $\pi(\bar{h}) \in H$.

Similarly, we note that for any $\bar{x} \in H + \bar{e}_i$, there is a permutation π such that $\pi(H) = H$ and $\pi(\bar{x}) \in H + \bar{e}_{m+1}$. □

Next we show that if the space L satisfies the conditions (D) and (A) then L cannot be a subspace of two distinct Hamming codes H_1 and H_2.

Lemma 6. *If L is a subspace of dimension $m - \log_2(m+1) - 1$ of two extended Hamming codes H_1 and H_2 of length $m+1$, then*

$$H_1 \neq H_2 \Longrightarrow Q(L) \text{ is not aperiodic}.$$

Proof. Assume that $H_1 \neq H_2$. Since L is the intersection of H_1 and H_2 and

$$\dim(L) = \dim(H_1) - 1 = \dim(H_2) - 1,$$

we may conclude that

$$\dim(H_1^\perp \cap H_2^\perp) = \dim(H_1^\perp) - 1 = \dim(H_2^\perp) - 1.$$

Without loss of generality, we may assume that the first $\log_2(m+1)$ rows of the matrix $\mathbf{Q}(L)$ in (10) belong to both $H_1^\perp$ and $H_2^\perp$, the last row $\bar{x}$ belongs to $H_2^\perp$, and the second to last row belongs to $H_1^\perp$.

As H_2 is a Hamming code, the relation below must hold for the word $\bar{x}$:

$$x_{2k} \equiv x_{2k-1} + 1 (\mathrm{mod}\ 2), \quad \text{for } k = 1, 2, \ldots, (m+1)/2.$$

As a similar condition holds for the entries in row number $\log_2(m+1)+1$, it is easy to see that the column

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & 0 & 1 & 1 \end{pmatrix}^{\mathrm{T}}$$

must be a period of the set of columns. □

In our algorithm to determine the number of equivalence classes, we make a list $\mathcal{L}$ of all subspaces of dimension $m - \log_2(m+1) - 1$ of a particular Hamming code H of length $m+1$ and satisfying the condition (A) above. We then consider the group $\mathcal{G}$ of permutations π that map subspaces of H of dimension $m - \log_2(m+1) - 1$ to other subspaces of H of the same dimension. According to Lemma 4, the number of orbits in $\mathcal{L}$ under $\mathcal{G}$ will be equal to the number of equivalence classes that we are looking for.

To determine the group $\mathcal{G}$, we use the following lemma.

Lemma 7. *If L is any subspace of dimension $m - \log_2(m+1) - 1$ of an extended Hamming code H of length $m+1$ such that the set $Q(L)$ is aperiodic, then for any permutation π of the set of coordinate positions,*

$$\pi(L) \subseteq H \Longrightarrow \pi(H) = H.$$

Proof. For any Hamming code H and any permutation π of the set of coordinate positions, the set $\pi(H)$ is a Hamming code. The space $\pi(L)$ is a subspace of the Hamming codes H and $\pi(H)$. Since the set $Q(L)$ is aperiodic, it follows from Lemma 6 that $H = \pi(H)$. □

The description of the set of permutations π such that for a given extended Hamming code H, $\pi(H) = H$, is well known and elementary, and is given by the use of the general linear group $GL(\log_2(m+1), 2)$, see [13].

As we now know the group $\mathcal{G}$, we can describe, by the use of a computer search, the set of orbits in $\mathcal{L}$ under this group. The computer search produced the following result.

Proposition 5. *The number of extended equivalence classes of perfect codes of rank $n - \log_2(n+1) + 1$ and with a kernel of dimension $n - \log_2(n+1) - \delta$ is equal to 5 for $\delta = 4$, and equal to 40 for $\delta = 5$.*

Let us remark that the result above can also be rather easily be checked by hand in the case $\delta = 4$.

In the Appendix, we explicitly describe all extended equivalence classes of perfect codes of length n, rank $n - \log_2(n+1) + 1$, and with kernels of dimension $n - \log_2(n+1) - 4$ and $n - \log_2(n+1) - 5$, respectively. They are described by their coset representatives $\bar{x}$, as in Lemma 5.

Appendix

This appendix contains two tables concerning subsets L of dimension $m - log(m+1) - 1$ of extended Hamming codes of length $m+1$, for $m+1$ equal to 16 and 32. The results were given by a computer search. The algorithm used for the computer search of the tables is described below:

$\mathcal{L}_0 = \{L \in \mathcal{L} \mid L = (\bar{x} + H^\perp) \quad \text{where } \bar{x} \in H \setminus H^\perp\}$
$\mathcal{L}_1 = \{L \in \mathcal{L} \mid L = (\bar{x} + H^\perp) \quad \text{where } \bar{x} \in H + \bar{e}_{m+1}\}$
$\mathcal{L}_2 = \{L \in \mathcal{L} \mid L = (\bar{x} + H^\perp) \quad \text{where } \bar{x} \in H + \bar{e}_{\{m,m+1\}}\}$
$\mathcal{G} =$ the set of permutations we get from $GL(\log_2(m+1), 2)$

while $\mathcal{L}_0 \neq \emptyset$ **do**
  $L \in \mathcal{L}_0$
  fixed = 0
  for each $\pi \in \mathcal{G}$ **do**
    $\mathcal{L}_0 \setminus \pi(L)$
    if $\pi(L)^\perp = L^\perp$ **then**
      $fixed = fixed + 1$
    end
  end
end
and similarly for $\mathcal{L}_1$ and $\mathcal{L}_2$.

Table 1
Extended equivalence classes, length 16.

Type	Class	Weight	Representation	|Fixed|
$\bar{x} \in H \setminus H^{\perp}$	1	6	0000001101010110	11 520
$\bar{x} \in \bar{e}_{16} + H$	2	1	0000000000000001	20 160
	3	3	0000000000001110	576
	4	5	0000110001011000	720
$\bar{x} \in \bar{e}_{\{15,16\}} + H$	5	4	0000000001010110	384

Table 2
Extended equivalence classes, length 32.

Type	Class	Weight	Representation	|Fixed|
$\bar{x} \in H \setminus H^{\perp}$	1	6	00000000000000000000001101010110	11 520
	2	8	00000000000000110000001101010101	1 152
	3	10	00000000000000110000010101101111	768
	4	10	00000000000000110101010101010110	4 032
	5	12	00000000000011111001100101010101	6 144
	6	12	00000000000101110001101101010110	1 920
$\bar{x} \in \bar{e}_{32} + H$	7	1	00000000000000000000000000000001	9 999 360
	8	3	00000000000000000000000000001110	64 512
	9	5	00000000000000000000000011110001	9 216
	10	5	00000000000000000000001110101000	1 920
	11	7	00000000000000000000000011111110	64 512
	12	7	00000000000000000000001100111110	768
	13	7	00000000000000000000001101010111	1 152
	14	7	00000011010101100000000000000001	720
	15	7	00000000000000110000001101010100	144
	16	9	00000011001111110000000000000001	768
	17	9	00000000000000110000001110101011	48
	18	9	00000000000000110000010101101110	48
	19	9	00000000110011110101000000001000	64
	20	9	01010101010101100000000000000010	1 008
	21	9	00000000000011000101010101011000	144
	22	11	00001001101011110011000000000001	192
	23	11	00110011001111000000000000001110	11 520
	24	11	00000000000011110011001101010100	192
	25	11	01010101010000100100111000000010	60
$\bar{x} \in \bar{e}_{\{31,32\}} + H$	26	4	00000000000000000000000001010110	9 216
	27	6	00000000000000000000001101010101	768
	28	6	00000000000001010001000100011000	720
	29	8	00000000000000000000000010101101111	1 024
	30	8	00000000000000000010101010101110	5 376
	31	8	00000000000000110000001101010110	192
	32	8	00000000000001010000010101010110	96
	33	8	00000000000001010001000100010111	72
	34	10	00000000000000110000010101011111	256
	35	10	00000000000000110101010101011010	768
	36	10	00000000000001010001000101111110	48
	37	10	00000000000001010011001100110101	576
	38	10	00000000000001010011010101100110	32
	39	10	01010101010000100100100001100000	120
	40	12	00000000000011110011001101010110	1 536

The different extended equivalence classes are given in the Tables 1 and 2. Every equivalence class is described by a word $\bar{x}$, as in (10), such that $L^{\perp} = H^{\perp} \cup (\bar{x} + H^{\perp})$. The minimum weight of the non zero words in the class is also given. By |Fixed|, we mean the number of permutations π in the algorithm in Section 5.4 that fix L.

References

[1] S.V. Avgustinovich, O. Heden, F.I. Solov'eva, On perfect codes ranks and kernels problem, Problems of Information Transmission 39 (4) (2003) 341–345.
[2] R.W. Hamming, Error detecting and error correcting codes, Bell System Technical Journal 29 (1950) 147–160.
[3] O. Heden, Perfect codes from the dual point of view I, Discrete Mathematics, in press (doi:10.1016/j.disc.2007.11.037).
[4] O. Heden, A full rank perfect code of length 31, Designs, Codes and Cryptography 38 (1) (2006) 125–129.
[5] O. Heden, A survey of perfect codes, Advances in Mathematics of Communications 2 (2) (2008) 223–247.
[6] O. Heden, M. Hessler, On the classification of perfect codes: Side class structures, Designs Codes and Cryptography 40 (2006) 319–333.
[7] F. Hergert, Algebraiche Methoden fur nichtlineare Codes, Thesis, Darmstadt, 1985.
[8] M. Hessler, Perfect codes as isomorphic spaces, Discrete Mathematics 306 (16) (2006) 1981–1987.

[9] M. Hessler, A Computer study of some 1-error correcting perfect binary codes, Australasian Journal of Combinatorics 33 (2005) 217–229.
[10] D.S. Krotov, Lower bounds on the number of m-quasigroups of order 4 and the number of perfect binary codes, Discrete Analysis and Operation Research 1 (7) (2000) 47–53. 2.
[11] P.R.J. Östergård, O. Pottonen, The perfect binary one-error-correcting codes of length 15: Part I - Classification, IEEE Trans. Inform. Theory (submitted for publication).
[12] K.T. Phelps, M. Villanueva, On perfect codes: Rank and kernel, Designs, Codes and Cryptography 27 (3) (2002) 183–194.
[13] N.J.A. Sloane, F.J. MacWilliams, The Theory of Error-correcting Codes, North-Holland, 1977.
[14] F.I. Solov'eva, On perfect codes and related topics, Com^{2}Mac Lecture Note Series 13, Pohang, 2004.
[15] Y.L. Vasil'ev, On nongroup close-packed codes, Problems of Cybernetics 8 (1962) 375–378.
[16] V.A. Zinoviev, D.V. Zinoviev, Binary perfect codes of length 16 by generalized concatenation construction, Problems of Information Transmission 38 (4) (2002) 56–84.
[17] V.A. Zinoviev, D.V. Zinoviev, Binary perfect codes of length 15 by generalized concatenation construction, Problems of Information Transmission 39 (1) (2003) 27–39.
[18] V.A. Zinoviev, D.V. Zinoviev, Binary extended perfect codes of length 16 and rank 14, Problems of Information Transmission 42 (2) (2006) 63–80.